***Formulaire des étapes à suivre***

**2e travail pratique du 2e semestre avec 15% d’influence sur la note de classe**

***Par TOKOBANZA EXAUCE***

**Matière : CRYPTOGRAPHIE Niveau : Dieux Durée : 03 jours**

* ***Pré – requis & calculs :***

On a déjà comme donnée l’adresse réseau principal (**192.178.12.0/24**) et le masque sou – réseau demandé est le /28.

* ***Calculs initiaux pour un sous – réseau /28 :***
* ***a. Le masque sous – réseau en notation décimale pointer pour un /28 :***

On a donc ceci : 255.255.255.240

* ***b. Nombre de bit allouer à la partie réseau et à la partie hôte :***

Pour la partie réseau on a **28 bits** qui y sont alloués et **4 bits** qui sont alloués à la partie hôte.

* ***C. Le nombre total d’adresse IP par sous – réseau :***

Par sous réseau on aura un total de **16** adresses.

* ***D. Le nombre d’hôtes utilisables :***

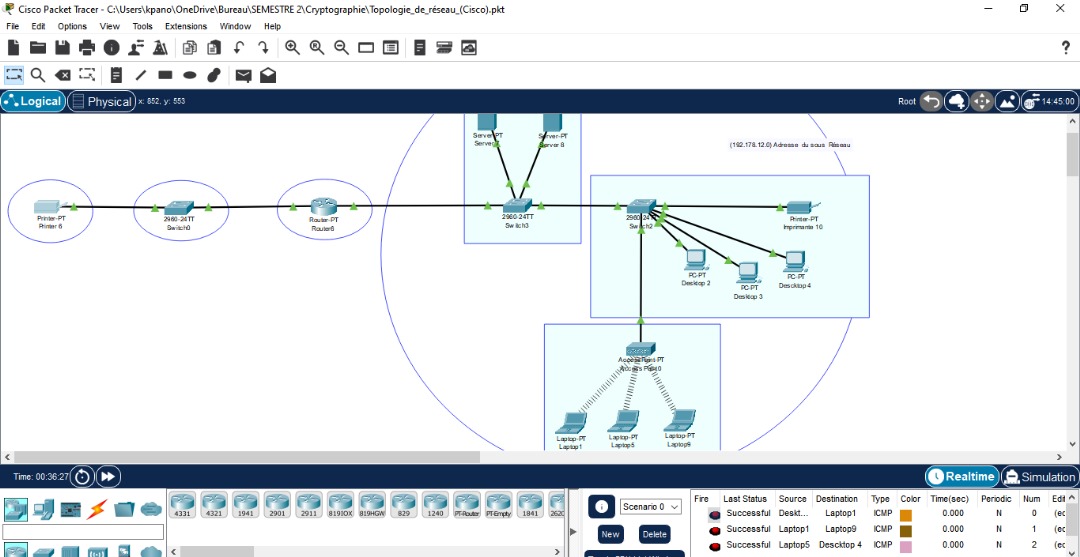
On a **14** hôtes utilisables d’une part on retient 1 pour l’adresse réseau et 1 pour le Broadcast.

* ***Les plages d’adresses pour les 4 premières sous – réseau :***

Avec l’adresse donnée 192.178.12.0/24, on va le couper en blocs de 16 adresses.

* ***Conception & implémentation du réseau :***
* ***Topologie du réseau :***
* ***Simulation du réseau :***

Avec l’utilisation du logiciel Cisco Packet Tracer.



* ***Indications des connexions entre les machines ou appareils :***
* Liaisons entre le switch2 et les trois desktops (2 ; 3 ; 4) ainsi que l’imprimante10
* Liaison entre le switch2 et un point d’accès
* Liaisons entre le point d’accès et les trois laptops (1 ; 5 ; 9)
* Liaison entre le switch2 et le switch3
* Liaisons entre le switch3 et les deux serveurs (Serveur A et Serveur B)
* Liaison entre le switch3 et un routeur (Routeur0)
* Liaison entre le routeur et le switch0
* Liaison entre le switch3 et l’imprimante6
* ***Plan des adressages :***

Des adressages statiques avec des adresses IP uniques et valides pour chacun des éléments.

* ***Test de connectivité :***

Vérification d’une connexion entre les machines.

* ***Détection et sécurit :***
* ***Détection des erreurs de configuration :***
* 192.178.12.0 : Adresse du réseau attribué au Laptop1 alors remplacement de l’adresse IP du Laptop1 par **192.178.12.2**
* 192.178.12.11 : Adresse IP appartenant au Laptop5 et au serveur B alors conservation de l’adresse pour le serveur B et remplacement de l’adresse IP du Laptop5 par **192.178.12.12**
  + - ***Finalisation du réseau :***
* La machine ne se trouvant pas dans le bon réseau est l’imprimante6
* Cette machine appartient au sous-réseau 2 dont l’adresse est **192.178.12.16** et l’adresse de broadcast est **192.178.12.31**
* ***Cryptographie :***
* ***Mise au point des indices donnés***
* Cryptage asymétrique
* Mode d’opération CBC en 256
* Clé : Le dernier octet en binaire de l’adresse broadcast de la machine infiltré du réseau avec **le préfix des deux premières lettres de l’adresse mac de l’ordinateur ayant pour adresse IP 182.216.58.64** du fichier de capture de wireshark transmis
* 31 en binaire donne : **00011111**
* Adresse MAC de l’ordinateur : **5c : 8c : 30 : 5e :77 : bc**
* La clé est donc : **cc00011111**
* ***Décryptage du fichier***
* Importation du fichier crypté de la machine hôte vers la machine virtuelle
* Décryptage du fichier et obtention du message caché.

**FIN DU TRAVAIL !!!!**